

The Claims

1. (Currently amended) One or more computer-readable media having stored thereon a plurality of instructions that, when executed by one or more processors of a computer, causes the one or more processors to perform acts including:

- allowing operation of the computer to begin based on untrusted code;
- loading, under control of the untrusted code, a trusted core into memory;
- preventing each of one or more central processing units and each of one or more bus masters in the computer from accessing the memory;
- resetting each of the one or more central processing units;
- allowing one central processing unit to access the memory and execute trusted core initialization code to initialize the trusted core; and
- after execution of the trusted core has been initialized, allowing any other central processing units and any bus masters in the computer to access the memory;

wherein the plurality of instructions further cause the one or more processors to perform acts including:

mapping a central processing unit reset vector to an initialization vector;

receiving a read request corresponding to the central processing unit reset vector from the one central processing unit;

returning, in response to the read request, the initialization vector to the one central processing unit; and

allowing the one central processing unit to access the memory beginning with the initialization vector.

2. (Original) One or more computer-readable media as recited in claim 1, wherein the one or more processors comprise one or more controllers of one or more memory controllers.

3. (Original) One or more computer-readable media as recited in claim 2, wherein the one or more memory controllers are distributed among the one or more central processing units.

4. (Original) One or more computer-readable media as recited in claim 2, wherein the plurality of instructions comprise microcode to be executed by the one or more memory controllers.

5. (Original) One or more computer-readable media as recited in claim 1, wherein the untrusted code includes code from a basic input output system (BIOS) and code from a plurality of option read only memories (ROMs).

6. (Original) One or more computer-readable media as recited in claim 1, wherein the preventing comprises preventing each of the one or more central processing units and each of the one or more bus masters from accessing the memory in response to an initialize trusted core command received from one of the one or more central processing units.

7. (Original) One or more computer-readable media as recited in claim 1, wherein the loading the trusted core comprises copying different portions of the trusted core from a plurality of different sources.

8. (Original) One or more computer-readable media as recited in claim 1, wherein the loading the trusted core comprises copying different parts of the trusted core from one or more sources and combining the different parts to assemble the trusted core.

9. (Previously presented) One or more computer-readable media as recited in claim 8, wherein combining the different parts comprises exclusive-ORing bits of the different parts.

10. (Original) One or more computer-readable media as recited in claim 1, wherein the loading the trusted core comprises copying at least a portion of the trusted core from a local mass storage device into the memory.

11. (Original) One or more computer-readable media as recited in claim 1, wherein the loading the trusted core comprises copying at least a portion of the trusted core from a remote device into the memory.

12. (Original) One or more computer-readable media as recited in claim 1, wherein the loading the trusted core comprises copying at least a portion of the trusted core from a chip of the computer.

13. (Original) One or more computer-readable media as recited in claim 1, wherein the preventing comprises ignoring all requests for access to the memory from the one or more central processing units and one or more bus masters.

14. (Original) One or more computer-readable media as recited in claim 1, wherein the plurality of instructions further cause the one or more processors to perform acts including:

extracting a cryptographic measure of the trusted core in the memory; and
storing the extracted cryptographic measure.

15. (Original) One or more computer-readable media as recited in claim 14, wherein the plurality of instructions further cause the one or more processors to perform acts including:

resetting a cryptographic processor;

requesting the cryptographic processor to extract the cryptographic measure; and

receiving the extracted cryptographic measure from the cryptographic processor.

16. (Original) One or more computer-readable media as recited in claim 1, wherein the resetting each of the one or more central processing units comprises asserting a processor bus reset signal to each of the one or more central processing units.

17. (Canceled).

18. (Currently amended) One or more computer-readable media as recited in claim 147, wherein the initialization vector is an address within the trusted core in the memory.

19. (Currently amended) One or more computer-readable media as recited in claim 147, wherein the plurality of instructions further cause the one or more processors to perform acts including:

re-mapping the central processing unit reset vector to an additional central processing unit start vector after returning the initialization vector to the one central processing unit; and

returning, in response to any other read request corresponding to the central processing unit reset vector from another central processing unit, the additional central processing unit start vector.

20. (Previously presented) One or more computer-readable media as recited in claim 19, wherein the initialization vector is an address within the trusted core in the memory and wherein the additional central processing unit start vector and the initialization vector are different addresses within the trusted core in the memory.

21. (Original) One or more computer-readable media as recited in claim 19, wherein both the initialization vector and the additional central processing unit start vector are obtained from the trusted core.

22. (Original) One or more computer-readable media as recited in claim 1, wherein the plurality of instructions further cause the one or more processors to perform acts including loading microcode from the trusted core in memory into the one central processing unit after resetting the central processing unit.

23-29. (Canceled).

30. (Previously presented) A method comprising:
booting, based on untrustworthy code, a computer;
loading a trusted core into memory; and

initiating secure execution of the trusted core by:

mapping a central processing unit reset vector to an initialization vector;

resetting each of one or more central processing units in the computer;

receiving, after the mapping and the resetting, a read request corresponding to the central processing unit reset vector from one of the one or more central processing units;

returning, in response to the read request, the initialization vector to the one central processing unit; and

allowing the one central processing unit to access the memory beginning with the initialization vector.

31. (Previously presented) A method as recited in claim 30, wherein the initialization vector is an address within the trusted core in the memory.

32. (Previously presented) A method as recited in claim 30, further comprising:

re-mapping the central processing unit reset vector to an additional central processing unit start vector after returning the initialization vector to the one central processing unit; and

returning, in response to any other read request corresponding to the central processing unit reset vector from another of the one or more central processing units, the additional central processing unit start vector.

33. (Previously presented) A method as recited in claim 32, wherein the initialization vector is an address within the trusted core in the memory and wherein the additional central processing unit start vector and the initialization vector are different addresses within the trusted core in the memory.

34. (Canceled).

35. (Canceled).

36. (Currently amended) A method comprising:
 allowing a computer to begin operation based on untrustworthy code;
 loading, under the control of the untrustworthy code, additional code into memory; and
 initiating execution of the additional code in a secure manner despite the untrustworthy code in the computer;
mapping a central processing unit reset vector to an initialization vector;
receiving a read request corresponding to the central processing unit reset vector from one central processing unit;
returning, in response to the read request, the initialization vector to the one central processing unit; and
allowing the one central processing unit to access the memory beginning with the initialization vector.

37. (Original) A method as recited in claim 36, wherein the initiating further comprises initiating execution of the additional code in a secure manner despite both the untrustworthy code in the computer and other pre-existent state of the computer.

38. (Currently amended) A method as recited in claim 36, wherein the initiating execution of the additional code in a secure manner comprises:

preventing each of one or more central processing units in the computer from accessing the memory;

preventing each of one or more bus masters in the computer from accessing the memory;

resetting each of the one or more central processing units;

allowing the one central processing unit to access the memory and execute a code initialization process; and

after execution of the code initialization process, allowing any other central processing units and any of the one or more bus masters to access the memory.

39. (Original) A method as recited in claim 36, wherein the initiating comprises initiating execution of the additional code in a secure manner without requiring any additional bus transactions to be supported by a processor in the computer.

40. (Canceled).

41. (Currently amended) A method as recited in claim 36[[40]], further comprising:

re-mapping the central processing unit reset vector to an additional central processing unit start vector after returning the initialization vector to the one central processing unit; and

returning, in response to any other read request corresponding to the central processing unit reset vector from another central processing unit, the additional central processing unit start vector.

42. (Canceled).

43. (Canceled).

44. (Original) A method as recited in claim 36, wherein the loading the additional code comprises copying different portions of the additional code from a plurality of different sources including one or more of: a local mass storage device, a remote device, and a local chipset.

45. (Canceled).

46. (Currently amended) A memory controller comprising:
a first interface to allow communication with a processor;
a second interface to allow communication with a system memory; and

a controller, coupled to the first interface and the second interface, to reset a processor and to allow the processor to execute a code initialization process while preventing any other processors from accessing the system memory;

wherein the controller is further to:

map a processor reset vector to an initialization vector;

receive a read request corresponding to the processor reset vector from the processor;

return, in response to the read request, the initialization vector to the processor; and

allow the processor to access the memory beginning with the initialization vector.

47. (Original) A memory controller as recited in claim 46, wherein the memory controller is included in a processor.

48. (Original) A memory controller as recited in claim 46, wherein the first interface comprises a processor bus interface.

49. (Original) A memory controller as recited in claim 48, wherein the memory controller operates without requiring the processor bus interface to support any additional commands on the processor bus.

50. (Original) A memory controller as recited in claim 46, wherein the system memory comprises a dynamic random access memory.

51. (Original) A memory controller as recited in claim 46, wherein the controller is further to allow the processor to execute the code initialization process while preventing any bus masters from accessing the system memory.

52. (Currently amended) A memory controller as recited in claim 46, wherein the controller is further to:

reset any other processor coupled to the memory controller prior to allowing the processor to execute the code initialization process;

prevent any other processor and any bus master coupled to the memory controller from accessing the system memory until the one processor executes the code initialization process; and

after execution of the code initialization process, allow any other central processing units coupled to the memory controller and any bus masters coupled to the memory controller to access the memory.

53. (Canceled).

54. (Currently amended) A memory controller as recited in claim ~~46~~⁵³, wherein the initialization vector is an address within the code initialization process.

55. (Currently amended) A memory controller as recited in claim 46~~53~~, wherein the controller is further to:

re-map the processor reset vector to an additional processor start vector after returning the initialization vector to the processor; and

return, in response to any other read request corresponding to the processor reset vector from another processor, the additional processor start vector.

56. (Original) A memory controller as recited in claim 55, wherein the initialization vector is an address within the code initialization process and wherein the additional processor start vector and the initialization vector are different addresses within the code initialization process.

57-61. (Canceled).

62. (Previously presented) An apparatus comprising:

a processor reset portion to assert a reset signal to a processor;

a memory protector portion to prevent any bus master from accessing memory until the processor completes execution of a trusted core initialization process; and

a controller, coupled to the memory protector portion, to:

map a processor reset vector to an initialization vector;

receive a read request corresponding to the processor reset vector from the processor;

return, in response to the read request, the initialization vector to the processor; and

allow the processor to access the memory beginning with the initialization vector.

63. (Original) An apparatus as recited in claim 62, wherein the controller is further to:

re-map the processor reset vector to an additional processor start vector after returning the initialization vector to the processor; and

return, in response to another read request corresponding to the processor reset vector from another processor, the additional processor start vector.

64-70. (Canceled).

71. (Previously presented) One or more computer-readable media as recited in claim 1, wherein the resetting comprises asserting, on a processor bus, a RESET# signal to each of the one or more central processing units.

72. (Previously presented) One or more computer-readable media as recited in claim 1, wherein the resetting comprises clearing a state of each of the one or more central processing units.

73. (Previously presented) One or more computer-readable media as recited in claim 72, wherein the state of a central processing unit comprises

instructions and data residing in any caches and buffers of the central processing unit.

74. (Previously presented) One or more computer-readable media as recited in claim 72, wherein the state of a central processing unit comprises instructions and data residing in any registers of the central processing unit.

75. (Previously presented) A memory controller as recited in claim 46, wherein the controller is to reset the processor by clearing a state of the processor.

76. (Previously presented) A memory controller as recited in claim 75, wherein the clearing the state of the processor comprises clearing all instructions and data from any caches or buffers of the processor.

77. (Previously presented) A memory controller as recited in claim 46, wherein the controller is to reset the processor by asserting, on a processor bus, a reset signal to the processor.

78. (Previously presented) A memory controller as recited in claim 77, wherein the reset signal comprises RESET#.

79-91. (Canceled).